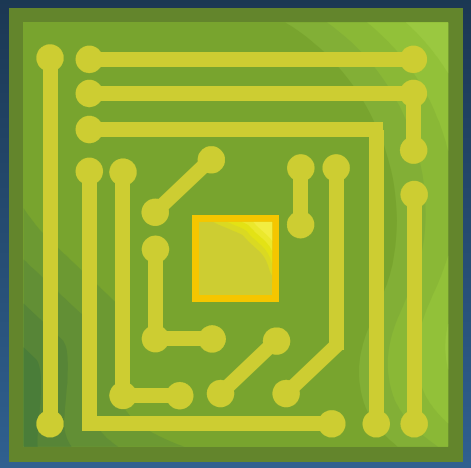
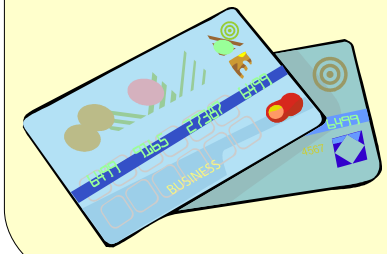
RFID Privacy and Authentication: An Overview

Ari Juels
RSA Laboratories

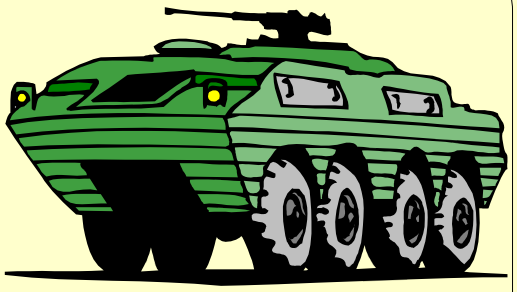


RFID underpins essential infrastructure

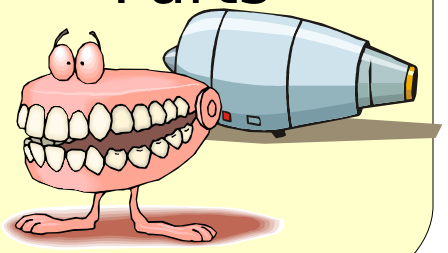
Payment devices



Materiel



Industrial & Medical Parts



Physical security

Border control

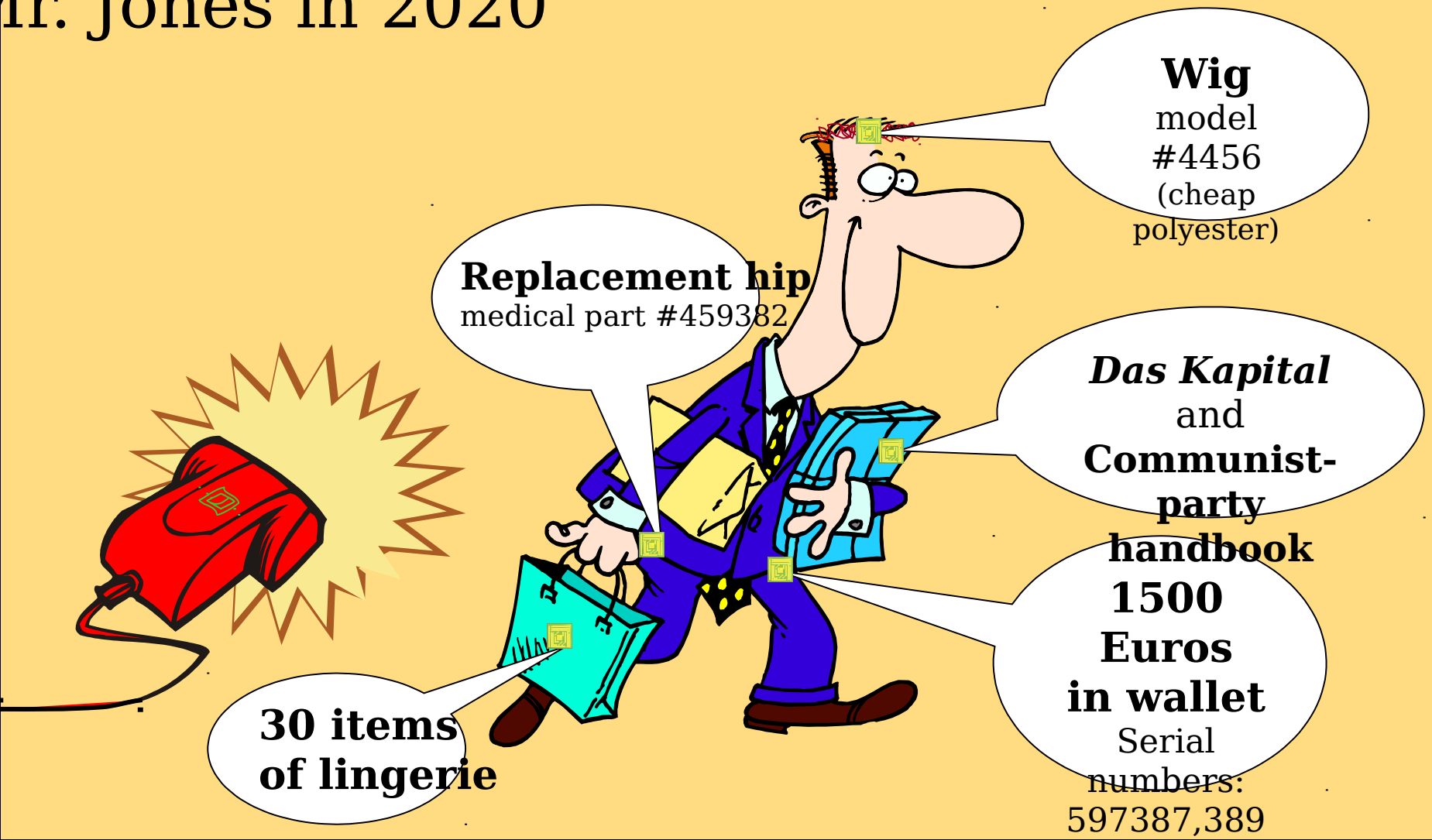
Food supply

Consumer goods

The privacy problem

Bad readers, good tags

Mr. Jones in 2020

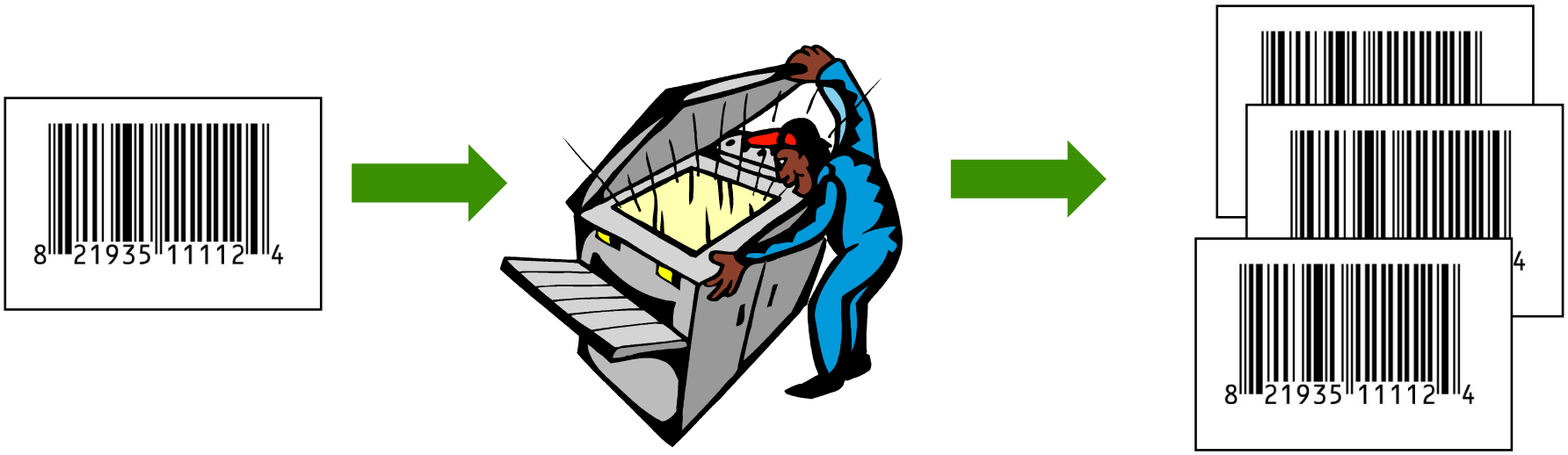


The authentication problem

Good readers, bad tags

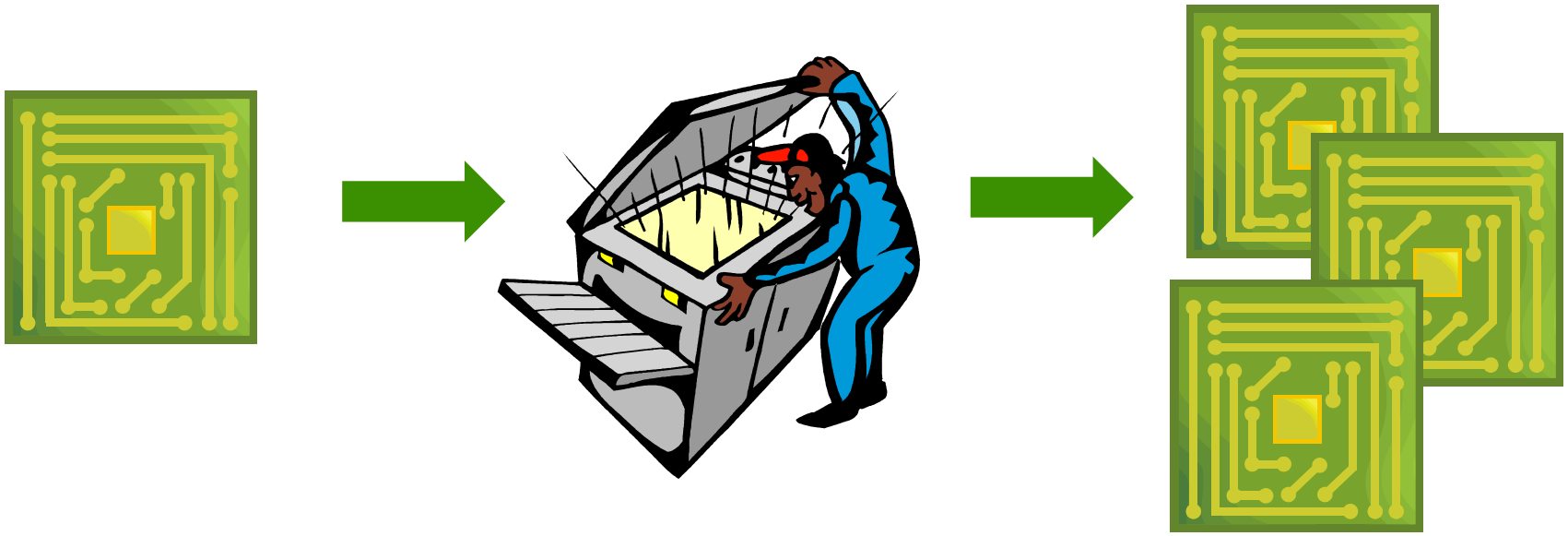
Where EPC tags fall short

- No explicit anti-counterfeiting features
  - An EPC tag is just a (wireless) barcode!



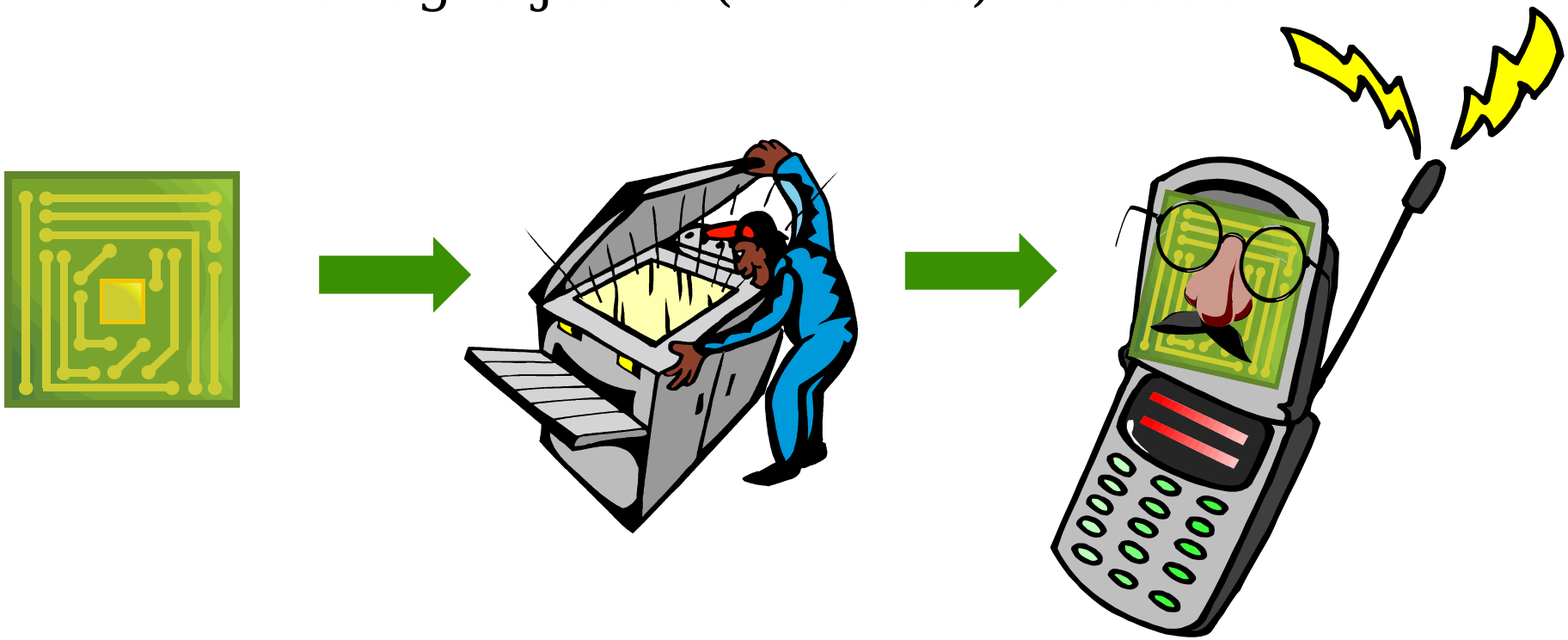
Where EPC tags fall short

- No explicit anti-counterfeiting features
  - An EPC tag is just a (wireless) barcode!

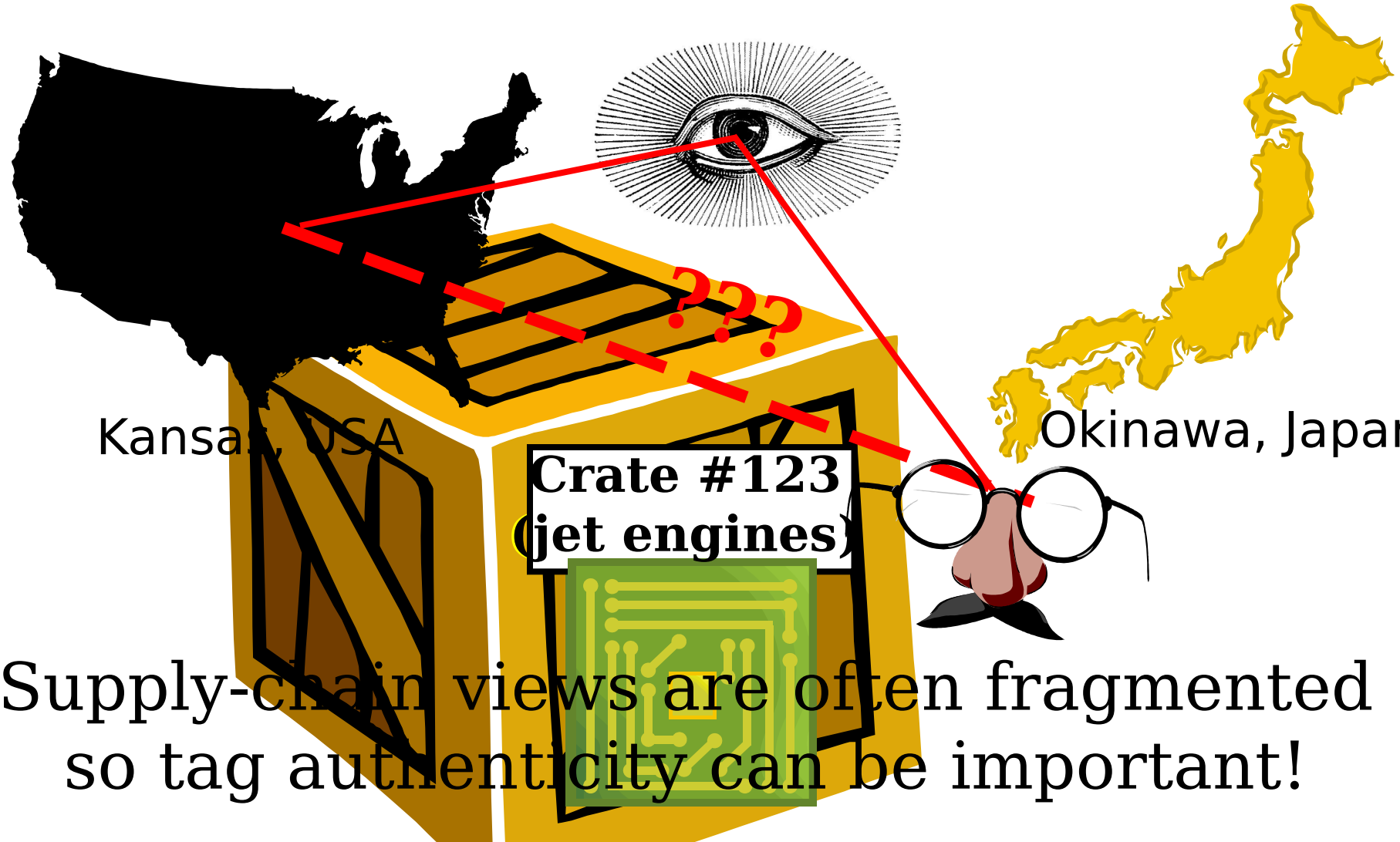


Where EPC tags fall short

- No explicit anti-counterfeiting features
  - An EPC tag is just a (wireless) barcode!



Why tag authentication matters

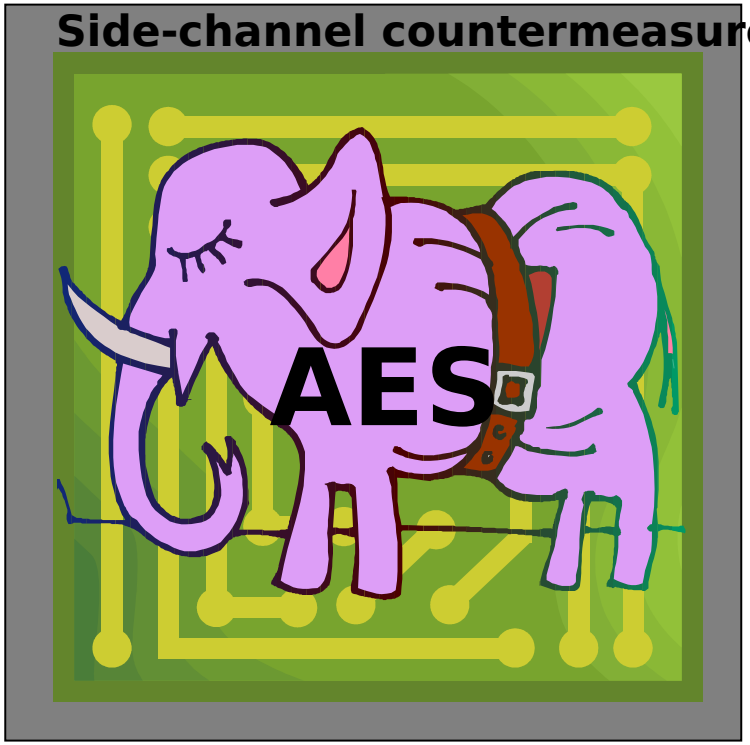


Supply-chain views are often fragmented so tag authenticity can be important!

EPC tags and privacy

- One true, explicit privacy feature: ***Kill***
  - **Dead tags** don't tell tales, but…
  - they don't confer post-sale benefits on consumers
  - they don't work in supply chains where privacy = security (e.g., military)
- Read-locking (soon to be introduced) can help somewhat with privacy and authentication…

Won’t “encryption” solve our problems?



We can do:

- Challenge-response for authentication
- Mutual authentication and/or encryption for privacy

But:

1. Moore’s Law vs. pricing pressure
2. Basic cryptography may not be enough because of problems of **key management…**

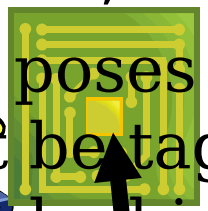
The key-management problem

Kansas, USA

Okinawa, Japan

The key poses “transport” problems:

- It must be tag-specific
- It must be highly available
- It must be secured at all times
- Like managing 10,000,000,000 passwords!



“Top secret: X-32 cone”

“Top secret: X-32 cone”

Conclusions

- RFID is creating infrastructure with critical security problems
  - Security/privacy are not optional
- Security is expensive as an afterthought
  - Today's Internet: phishing, pharming, spam, etc…
  - Today's choices will determine tomorrow's RFID security
  - Standards bodies must draw on right expertise (recall 802.11)
- System- and supply-chain- fragmentation are defining features of security landscape
  - Policy solutions are hard because of multiplicity of stakeholders, e.g., privacy
  - "Encryption" is not a cure-all (nor it is always the right choice)
- Security and privacy are *enablers*:
  They create conditions to unlock the potential of RFID